CLAIMS

What is claimed is:

1. A method of providing data from a service to a client over a telecommunication network based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

selecting a service that can provide the data to the client, based on matching the list of encryption types received from the client to a mapping of encryption types to available services; and

causing communication of the data from the selected service to the client.

2. A method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step.

3. A method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the secure connection is established using a security protocol selected from among the set consisting of SSL, PPTP, SSH, and IPSec.

4. A method as recited in Claim 9, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, wherein the step of establishing the secure connection further comprises the step of establishing the secure connection with the client using a cipher suite match.

5. The method as recited in Claim 1, further comprising the step of establishing a secure connection with the client, and wherein the receiving step is carried out as part of the establishing step, and further comprising the step of disconnecting the secure connection and reestablishing the secure connection using a cipher suite match.

6. The method as recited in Claim 1, wherein the ordered mapping of encryption types to services is an ordered mapping of cipher suites to services.

7. The method as recited in Claim 1, further comprising the steps of receiving a weight value for one or more of the encryption types, and ordering the mapping of encryption types to services based on the received weight values.

8. A method as recited in Claim 1, wherein the encryption type is a cipher suite match.

9. A method as recited in Claim 1, wherein the step of determining the service further comprises the steps of:

determining an encryption type match by finding a first common encryption type in the list of encryption types and the mapping of encryption types to services;

transmitting the encryption type match to the client;

selecting a service associated with the encryption type match;

selecting a server farm based on the service; and

selecting a particular server in the server farm to provide the data to the client.

10. A method as recited in Claim 1, wherein the step of causing communication further comprises the step of establishing a connection with a non-encrypted protocol for use in communicating a request to the selected service to cause communication of the data from the selected service to the client.

12. A method as recited in Claim 1, wherein the mapping of encryption types to services is stored in an SSL termination module.

13. A method of providing data associated with a service to a client over a telecommunication network based on SSL encryption capabilities of the client, the method comprising the computer-implemented steps of:

creating and storing, at an SSL termination device, a mapping that associates cipher suites that are supported by the SSL termination device with services that are accessible through the SSL termination device;

receiving from the client as part of an SSL handshake phase message, a request for data and a list of cipher suites that are available at the client;

matching the cipher suite list received from the client to the mapping to result in identifying at least one cipher suite in common between the cipher suite list and the mapping;

identifying, from the mapping, a service corresponding to the cipher suite in common; and

causing communication of the data from the selected service to the client over an SSL connection using encryption parameters as defined in the cipher suite in common.

14. A method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

transmitting to an endpoint a request for data and an ordered list of encryption types that correspond to encryption types that are available at the client;

receiving from the endpoint an encryption type; and

receiving data that corresponds to the request from the service that is selected based on the encryption type.

15. A method as recited in Claim 14, further comprising the step of establishing a secure connection between the client and the endpoint, wherein the secure connection is established using a security protocol consisting of SSL, PPTP, SSH, and IPSec.

16. A method as recited in Claim 15, wherein the step of establishing the secure connection further comprises the step of establishing the secure connection between the client and the endpoint using a cipher suite match.

17. The method as recited in Claim 15, further comprising the step of disconnecting the secure connection and reestablishing the secure connection using a cipher suite match.

18. The method as recited in Claim 15, wherein the endpoint is a SSL termination device.

19. The method as recited in Claim 15, wherein the ordered list of encryption types is an ordered list of cipher suites.

20. A method as recited in Claim 19, wherein the encryption type is a cipher suite match.

21. A computer-readable medium carrying one or more sequences of instructions for providing data from a service to a client based on encryption capabilities of the client, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

transmitting to an endpoint a request for data and an ordered list of encryption types that correspond to encryption types that are available at the client;

receiving from the endpoint an encryption type; and

receiving data that corresponds to the request from the service that is selected based on the encryption type.

22. A computer-readable medium carrying one or more sequences of instructions for providing data from a service to a client based on encryption capabilities of the client, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

selecting a service that can provide the data to the client, based on matching the list of encryption types received from the client to a mapping of encryption types to available services; and

causing communication of the data from the selected service to the client.

23. An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

means for transmitting to an endpoint a request for data and an ordered list of encryption types that correspond to encryption types that are available at the client;

means for receiving from the endpoint an encryption type; and

means for receiving data that corresponds to the request from the service that is selected based on the encryption type.

24. An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

transmitting to an endpoint a request for data and an ordered list of encryption types that correspond to encryption types that are available at the client;

receiving from the endpoint an encryption type; and

receiving data that corresponds to the request from the service that is selected based on the encryption type.

25. An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

means for receiving from the client a request for data and a list of encryption types representing encryption capabilities that are available at the client;

means for selecting a service that can provide the data to the client, based on matching the list of encryption types received from the client to a mapping of encryption types to available services; and

means for causing communication of the data from the selected service to the client.

26. An apparatus for providing data from a service to a client based on encryption capabilities of the client, comprising:

a network interface that is coupled to a data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

receiving from the client a request for data and an ordered list of encryption types;

determining a particular server to retrieve the data based on the ordered list of encryption types and an ordered mapping of encryption types to services; and

causing communication of the data from the particular server to the client.

27. A method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

receiving an ordered list of cipher suites that corresponds to cipher suites available to a client;

establishing an SSL connection with an SSL termination module;

transmitting to the SSL termination module a request for data and the ordered list of cipher suites;

receiving from the SSL termination module a cipher suite match

establishing an new SSL connection with the SSL termination module using the cipher suite match; and

receiving data that corresponds to the request

wherein the data is retrieved from a service that is selected based on the cipher suite match.

28. A method of providing data from a service to a client based on encryption capabilities of the client, the method comprising the computer-implemented steps of:

receiving an ordered mapping of cipher suite names to services;

receiving from the client a request for data and an ordered list of cipher suites;

determining a cipher suite match by selecting a first common cipher suite in the ordered list of cipher suites and the ordered mapping of cipher suite names to services;

transmitting the cipher suite match to the client;

selecting the service associated with the cipher suite match;

selecting a server farm based on the service;

selecting a particular server in the server farm to provide the data to the client; and

transmitting the data to the client.